UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/756,456	01/08/2001	Arif Askerov	2003453-0001	5553

7590 07/29/2004

Sam Pasternack
Choate, Hall & Stewart, Exchange Place
Exchange Place
53 State Street
Boston, MA 02109-2891

EXAMINER
SEAL, JAMES

ART UNIT	PAPER NUMBER
2135	8

DATE MAILED: 07/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/756,456	**Applicant(s)** ASKEROV ET AL.	
	Examiner James Seal	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-91* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-91* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This correspondence is in response to applicant's correspondence of 08 January 2001.

2. The IDS dated 08 February 2002 has been considered and a sign copy enclosed with this correspondence.

3. Claims 1-91 are pending.

Oath/Declaration

It does not state that the person making the oath or declaration has reviewed and understands the contents of the specification, including the claims, as amended by any amendment specifically referred to in the oath or declaration.

It does not state that the person making the oath or declaration acknowledges the duty to disclose to the Office all information known to the person to be material to patentability as defined in 37 CFR 1.56.

Specification

4. The disclosure is objected to because of the following informalities: For example the term "firmness" in line 3 line 9 should be "security". The applicants are responsible for proofing their specification.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-9, 11-91 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gutowitz US 5365589 A and further in view of Campinos et. al. US 6091818 A, and Serpell US 4633037 A.

6. As per claim 1, the limitation of converting a binary sequence (input binary stream Figure 1 element) into a final encrypted content (Figure 1, ciphertext), Further Gutowitz teaches a conversion function (Figure 1, element 400, which is any finite state machine which is selected from a predefined set including classical encryption function such as DES or chaotic system based on say the logistic equation or cellular automata (Column 1, lines 16-43). The algorithm (state evolution function) is any algorithm or algorithms with good mixing properties (Column 10, lines 11-17) over a selected number of iteration say P (Column 3, lines 28-31). Gutowitz further teaches selecting an alphabet see Column 11 lines 45-46; and Table I is given as an example. Finally Gutowitz teaches encryption by selectable external keys from a very large set (Column 3, lines 59-60). Gutowitz is silent on Tag data and structure data.

7. Campinos discloses extraction of identifier DX1 = I(K1), DX2, ... DXn and create a tagged data T (see Campinos Figure 3a, Column 5, lines 14-21)

$$T = \{DX1, DX2, \dots\}$$

which forms a transformed data structure, the transformation being an encryption algorithm E applied to content data CW1, CW2, ... using keys K1, K2, ... and forming the structure data set S

$$S = \{ A1 = E(CW1)_{K_1}, A2, \dots \}$$

the elements of the sequence A1, A2, ... of logical scales of position coding (certainly the encryption algorithm forms a position coding of the content CW1, CW2, ... CWi, where i denotes the position in the sequence, E is an encoding process, and length of the data blocks, number of blocks, and keys such that the key size increases (scales) with the rank of the key K so as to make pirating increasingly difficult, Column 7, lines 1-2, Column 9, lines 19-20) which is then concatenated into C2a

C2a = { T, S}

It would have been obvious for one of ordinary skill in the art at the time the invention was made to have modified Gutowitz (symmetric encryption/decryption system with selectable encryption algorithm and selectable number of iteration, which keys each block with a different keys) with Campinos teaching of tagging because the combination would provide a means of transporting key data across communication links. encryption/decryption system with selectable encryption algorithm and selectable number of iteration, which keys each block with a different keys) with Campinos teaching of tagging days as a means of transporting for example the key data across communication links.

8. The Gutowitz/Campinos combination does not specifically mention the encryption of the tags. Serpell teaches the use of encrypting tags (tokens) which are used identify transaction keys at both the retailer store and the bank so that the transaction can be carried out using the transaction key. Note the transaction key is never transferred but the encrypted token is used to identify the key at the customer's bank. Note it is the bank's key (the external key K^x) that encrypts the token *T"*, which is known at both the

node and the bank (i.e. the retailer's key). Thus Serpell teaches encrypting label (or tags or token) so that the proper key (the transaction key) can be identified by the bank (and the merchant) see Figure 3 and 4 and Column 5, lines 28, 35-36, 60-67 Column 6, line 1. Thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the Gutowitz/Campinos combination because it allows the key the identification of the key through the key tag without an attacker on the communication link to know which key might be used. Which would yield the encrypted final image G as a concatenation of the coded tag data elements and the transformed structure elements S' upon the Pth iteration of the algorithm. Claim 1 is rejected.

9. The limitations of claim 2, differ from those of claim 1 in that the internal key is defined by use of Stochastically selected (i.e. randomly selected) bits is disclosed by Gutowitz (Column 3, lines 59-60). The limitation of converting a binary sequence (input binary stream Figure 1 element) into a final encrypted content (Figure 1, ciphertext). Gutowitz is silent on determining whether to extract internal identifiers and if so forming in a internal identifier file FID.

10. Campinos discloses extraction of identifier DX1 = I(K1), DX2, ... DXn but the identifier are dependent on the content to be transmitted. Thus a determination on a case by case basis of what identifier to extract dependent on the content. The extracted data is put into a file

$$T = \{DX1, DX2, \dots\}$$

which we can placed in a file called FID as it is a file containing extracted identifiers (Column 4, lines 23-25).

11. It would have been obvious for one of ordinary skill in the art at the time the invention was made to have modified Gutowitz (symmetric encryption/decryption system with selectable encryption algorithm and selectable number of iteration, which keys each block with a different keys) with Campinos teaching of extracting only those identifiers needed because of the need for decreasing bandwidth. Claim 2 is rejected.

12. The limitations of claim 3, differ from those of claim 2 in that the internal identifiers are partially encoded. Gutowitz teaches partially (or selectively) encrypting (encoding) (Column 35, lines 37-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined the teaching of Gutowitz partial encryption with those of Campinos of tagged data because partial encryption of data would allow restriction of who gets to see the information Those having a key to decrypt it while all others would only be able to view a part of the document or data being transmitted (Column 1, lines 66-68 and continuing top Column 2, line 4). Further, partial encryption allows conservation of bandwidth and finally in certain e-commerce application, partial such as pay per view.

13. Thus the partially encrypted tag file now denoted as T" we can combine it with the structure elements to obtain the encrypted final image G as a concatenation of the coded tag data elements and the transformed structure elements S" upon the Pth iteration of the algorithm. Claim 3 is rejected.

14. As per claim 4, the limitations of claim 2, with the additional limitation of converting the FID field with an external key (Serpell's external key) selected

stochastically (randomly) is taught by Gutowitz (Column 3, lines 59-60). Claim 4 is rejected.

15. As per claim 5, the limitation that the external key K^x is selected from a plurality of external keys K_{EXT} is disclosed in Gutowitz Column 3, lines 16-17. Claim 5 is rejected.

16. As per claim 6, the limitation of selection of K^x based on random means is disclosed by Gutowitz (Column 3, lines 59-60). It would have been obvious for one of ordinary skill in the art at the time that the invention was made to have modified the combination Gutowitz/Campinos, and Serpell because keys obtained from random sources have greater security. Claim 6 is rejected.

17. As per claims 7-8, the limitation that the external key K^x used by the encryption algorithm of each round is a is either the same for all iteration or different is disclosed by Gutowitz . Gutowitz discloses (Column 20, lines 27-50) that the level of security desired is connected with the key management. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have invoked a key management of using the same key for all rounds for low level security and different keys for each round for a higher level level of security, because over use of a key will make the corresponding cipher less secure. Thus one might use the same key for all iteration for low security traffic and a different key for each iteration for a secure cipher. Claims 7-8 are rejected.

18. As per claim 9, the limitation that the external key K^x is user supplied by the user. Gutowitz teaches (Column 36, lines 13-16) in a shared key K encryption between

user A and B, if A wishes to send a message M to B, they encrypt it E_K hence Gutowitz teaches that the user supplies the key. Claim 9 is rejected.

19. As per claims 11-15, the limitation that the choice of transformation algorithm is selected based upon a random choice, logic, mathematical, file size, or user predetermined criterion. Gutowitz further suggest the use of *mathematical criterion* to define the transformation algorithm for example using the *logistic map* (Column 21, lines 42). Gutowitz discloses transformations based on *mathematical logic*, in particular the XOR (Column 18, lines 16-25). Gutowitz also discloses in *stochastic* (random or arbitrary) selection of the toggle rules when the states are defined by cellular automaton rather than chaotic states (Column 25, lines 38-43). Gutowitz teaches that the transformation (rule) may be selected based on the size of the lattice or system (which would be in turn decided on the size of the data to be transmitted and hence the size of the file) to be transformed (Column 27, lines 20-31). Claims 11-15 are rejected.

30. As per claims 16-19, the limitation that the number of iterations is a feature which is selected is Gutowitz (Column 3, lines 28-29). That the criterion for selection is based on randomness, a mathematical criterion, a logical criterion, or dependent on the file size would be in keeping with the method of choice of the algorithm. See claims 11-15. Claims 16-19 are rejected.

31. As per claim 20, the limitation that the quant comprise a segment of structural data element S is taught by Gutowitz. Table 1 illustrates encode letters into segments of structural data that is X is mapped into data structure 1011. Claims 20 is rejected.

32. As per claims 21-22, the limitation of determining upon which iteration whether there internal idenitifiers and if any extracted is taught by the combination Gutowitz/Campinos. Campinos (Column 4, lines 23-24) teaches the extraction of internal identifies depend upon the information requested by the user. Gutowitz teaches that the number of iterations can be dependent upon the desired security level (Column 3, lines 27-28). Hence the number of iteration is dependent on the security level of the data and thus the number of iteration determines the number of iterations. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Gutowitz with Campinos because if the data being transferred were sensitive, more iterations would be needed, and the extraction of such identifier would be necessary. Claims 21-22 are rejected.

33. As per claims 23-26, the limitation that the number of bits per character respresentation is a feature which is selected is Gutowitz (Table 1). That the criterion for selection is based on randomness, a mathematical criterion, a logical criterion, or dependent on the file size would be in keeping with the method of choice of the algorithm. See claims 11-15. Claims 23-26 are rejected.

34. As per claim 27, the limitation to reverse the process of claim 1 is taught by the combination Gutowitz /Campinos /Serpell as Gutowitz teaches both encryption as well as decryption (which is the reverse of the first) and thus is rejected in view of the same prior art of record.

35. As per claims 28-29, the limitation of an indicator (counter) as to whether the Pth iteration has been reached is taught by Gutowitz /Campinos /Serpell as the very

process of reversing (decrypting) would require undoing the iteration and hence must require knowing (an indicator or counter) and performing that many iterations and thus is rejected in view of the same prior art of record.

36. As per claim 30, the limitation that the scrambling function is selected from a scrambling matrix (= Array) of predefined scrambling functions (= rules) is disclosed by Gutowitz (Column 12 lines 6). Claim 30 is rejected.

37. As per claim 31, the limitation that the predefined set of scrambling functions are changed is disclosed by Gutowitz (Column 20, lines 15-17). Gutowitz is silent on changing the automaton rules periodically, however, one of ordinary skill in the art would realize that with the large number of possible rules at hand that changes on a periodic basis is the easiest method to insure security. Claim 31 is rejected.

38. As per claims 32-34, the limitation of inserting user information into the structural data to provide both authentication and digital signing is disclosed by Gutowitz (Column 37 lines 67 and Column 38 lines 1-2). Claims 32-34 is rejected.

39. Claims 35-61 recites a computer executable process with steps stored on a computer readable medium for performing method claims 1-3, 5-9, 11-20, 23-31 and are rejected in view of the same prior art of record.

40. Claims 62-91 recites an apparatus for performing method claims 1-20, and 23-31 and are rejected in view of the same prior art of record.

41. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Campinos et. al. US 6091818 A, and further in view of Gutowitz US 5365589 A, Serpell US 4633037 A and Ichikawa US 5872846 A.

42. As per claim 10, the limitation of claim 5, wherein the external keys file is converted using transformations and then transmitted to the subscriber. Ichikawa teaches encrypting the keying material and then transmitting it to the user(s) see Figure 3 and Column 5 line 21-22. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the combination Gutowitz, Campinos, and Serpell to have supplied keys for rekeying remote subscriber by using key-encrypt-key (KEK) techniques, because it provides a method of distributing keys to remote users without jeopardizing the security of the keys or the content they will encrypt. Claim 10 is rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

James Seal

James Seal
Examiner 2135
22 July 2004